Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)92

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Frau Dagmar Hartge

Fragenkatalog

für das Fachgespräch zur „EU-Datenschutz-Grundverordnung“

des Ausschusses Digitale Agenda am 24. Februar 2016 im Deutschen Bundestag

1) Wie sind die Ergebnisse des Trilogs zur Datenschutz-Grundverordnung aus Ihrer Sicht grundsätzlich zu bewerten?

Die Ergebnisse bewerte ich nach den jahrelangen Verhandlungen im Großen und Ganzen als Erfolg. Ich freue mich, dass es in zentralen Punkten im Trilog-Verfahren noch zu Einigungen gekommen ist, die das Grundrecht auf Datenschutz stärken. Nennen möchte ich hier zum einen die Zweckbindung, die am Ende nicht so stark wie es vorgesehen war eingeschränkt worden ist und zum anderen den Grundsatz der Datensparsamkeit (Datenminimierung), Artikel 5 Abs. 1c Datenschutz-Grundverordnung (DSGVO), der ein zentraler Ansatz des Datenschutzrechts ist, da er unmissverständlich zeigt, dass nur die tatsächlich erforderlichen Daten auch durch Dritte verarbeitet werden dürfen.

Ob die Datenschutz-Grundverordnung ihre Versprechen in allen Bereichen halten kann, wird sich erst in der Anwendung zeigen. Es wird darum gehen, die unbestimmten Rechtsbegriffe und die allgemeinen Regelungen mit Leben zu erfüllen. Genau an dieser Stelle wird es noch einmal sehr spannend werden. Aus diesem Grund ist auch die Zweijahresfrist bis zur Anwendung der DSGVO sehr wichtig. Sie muss genutzt werden, um Ausführungsvorschriften, innerstaatliche Rechtsvorschriften und verbindliche Regelungen für die Zertifizierung und Akkreditierung zu erarbeiten. Die nationalen Gesetzgeber, der Europäische Datenschutzausschuss und die Europäische Kommission sind an dieser Stelle gefragt.

Im Zusammenhang mit der Datenschutz-Grundverordnung sind Big Data, Ubiquitous Computing, Cloud Computing und andere datenzentrierte Geschäftsmodelle diskutiert worden. Sind diese Möglichkeiten der modernen Datenverarbeitung - vor dem Hinter-grund der getroffenen Regelungen zur Weiterverarbeitung und Pseudonymisierung - aus Ihrer Sicht weiterhin möglich.

Ja, diese Geschäftsmodelle sind möglich und werden auch in Zukunft möglich sein. Die Datenschutz-Grundverordnung enthält ausreichend viele Ansätze, die der Wirtschaft hier die Richtung weisen. Zum einen sieht die DSGVO zum ersten Mal die Verpflichtung zur Umsetzung von „Privacy by Design“ vor. Zum anderen ist bei jeder Produktentwicklung das Datenschutzrecht des Einzelnen bereits frühzeitig zu berücksichtigen. Mit Hilfe von Anonymisierungen und Pseudonymisierungen lassen sich diese Geschäftsmodelle erfolgreich entwickeln.

Im Übrigen sehe ich in dem strikten Ansatz der DSGVO, mehr Transparenz bei der Datenverarbeitung vorzuschreiben, einen wichtigen Ansatz für die Zukunft. Bisher wird immer unterstellt, dass die Bereitschaft der Menschen, Daten für Big Data Zwecke zur Verfügung zu stellen, nicht gegeben sei. Mit mehr Transparenz und besserer und verständlicherer Aufklärung darüber, was bei der Verarbeitung tatsächlich gemacht wird und welche Risiken es gegebenenfalls gibt, wird es mehr Menschen geben, die bereit sind, Vorhaben und Entwicklungen der Wirtschaft zu unterstützen. Darin sehe ich auch eine Chance. Wichtig ist es, hohe Datensicherheitsstandards vorzusehen und umzusetzen, um eine höchstmögliche Minimierung der Risiken für den Einzelnen zu erreichen. Außerdem sollte es auch ethische Grenzen geben, die im Hinblick auf die Persönlichkeitsrechte jedes Einzelnen nicht überschritten werden dürfen.

Welche Auswirkungen auf den internationalen Wettbewerb sind für europäische Anbieter zu erwarten?

Für europäische Unternehmen sehe ich keine negativen Auswirkungen auf dem internationalen Markt. Die DSGVO hat mit dem Marktortprinzip für europäische Unternehmen in Europa eine Gleichheit mit Unternehmen aus Drittstaaten hergestellt, die wir vorher nicht hatten. Umgekehrt ist für europäische Unternehmen auf den internationalen Märkten ein hohes Datenschutzniveau kein Nachteil. Das Problem lag in der Vergangenheit vor allem darin, dass große amerikanische Unternehmen, die Produkte und Dienstleistungen in Europa anbieten, sich nicht an die europäischen Regelungen der Datenschutzrichtlinie gehalten haben. Dies wird jetzt anders werden. Hinzu kommt, dass der europäische Markt für diese Unternehmen wirtschaftlich nicht unbedeutend ist, so dass seine Regeln wahrscheinlich auch vor diesem Hintergrund, sowie der nun höheren Sanktionsmöglichkeiten, Beachtung finden werden. Ein gutes Beispiel für die Bedeutung des europäischen Marktes für US-amerikanische Unternehmen ist das Unternehmen Microsoft, das mit T-Systems in Deutschland kooperiert.

Inwiefern wird die DSGVO den gestiegenen Herausforderungen hinsichtlich eines effektiven Grundrechtschutzes angesichts neuer Arten der Datenerfassung, Speicherung, Verarbeitung und Weitergabe an Dritte insgesamt gerecht?

Die DSGVO enthält zahlreiche Regelungen, die gut geeignet sind, einen effektiven Grundrechtsschutz für die Betroffenen zu gewährleisten. Da es bei den technischen Regelungen jedoch regelmäßig noch der Ausführungsvorschriften bedarf, kann hier nur eine erste Einschätzung gegeben werden.

Angesichts der rasanten technischen Entwicklung kommt der Sicherheit der Datenverarbeitung für die Umsetzung des Grundrechts auf Datenschutz die herausragende Rolle zu. Besonders wichtig sind daher Art. 23 und 30, die Datenschutz durch Technik, datenschutzfreundliche Voreinstellungen sowie allgemeine Regelungen für die Sicherheit der Verarbeitung treffen. Diese Vorschriften sind, um technikneutral zu sein, nicht sehr detailliert. Hier kommt es also darauf an, mit welchen detaillierten Vorgaben diese Regelungen umgesetzt werden.

Die Betroffenen profitieren auch von Art. 33, der für Datenverarbeitungen mit einem hohen Risiko eine vorherige „Datenschutz-Folgenabschätzung" verbindlich regelt und hierbei die vorherige Konsultation der zuständigen Aufsichtsbehörde verpflichtend macht. Gerade neue Formen der Datenverarbeitung tragen oft ein hohes Risiko in sich. Diese kommen an einer vorherigen intensiven Prüfung nicht vorbei. Auch Datenschutzzertifizierungen, wie sie Art. 39 und 39a regeln, sind für den Betroffenen ein Vorteil, da sie eine Prüfung der Datenschutzanforderungen nach festgelegten Prüfanforderungen garantieren. Voraussetzung ist hier, dass sich qualitativ gute Datenschutzzertifizierungen etablieren.

Effektive Regelungen für Betroffene sind auch Art. 17, der das sog. Recht auf Vergessen, also Löschungsrechte der Betroffenen enthält sowie Art. 18 mit dem für die Betroffenen neuen Recht auf Datenportabilität.

Artikel 20 regelt das sog. Profiling. Die Profilingregelung ist bedauerlicherweise sehr unkonkret. Sie verzichtet darauf, im Gesetz eindeutige Grenzen für ein Profiling zu regeln. Es bleibt abzuwarten, ob sie die Erwartung, durch eine gesetzliche Regelung eine Verbesserung der Betroffenenrechte zu erreichen, tatsächlich erfüllen kann.

Die Transparenzregelungen des Art. 12 und die Informations- und Auskunftsrechte in Art. 14, 14a und 15 sind für einen funktionierenden Grundrechtsschutz wesentlich. Nur derjenige, der gut und nach seinem Verständnis auch ausreichend über die Verarbeitung seiner personenbezogenen Daten informiert wird, kann sein informationelles Selbstbestimmungsrecht tatsächlich selbstbestimmt nutzen. Gerade die Transparenz war in der Vergangenheit häufig mehr als mangelhaft. Hier sind Verbesserungen und Weiterentwicklungen für die Betroffenen besonders wichtig.

Die DSGVO enthält damit wichtige Ansätze für einen effektiven Betroffenenschutz. Nun kommt es darauf an, dass diese Ansätze auch genutzt und die Vorschriften mit

Leben erfüllt werden. Insofern liegt nach der Verabschiedung der DSGVO die wichtige Umsetzungsarbeit noch vor uns. Erst nach dieser Arbeit kann beurteilt werden, ob die mit der DSGVO verbundenen Chancen genutzt worden sind.

2) Wird mit der Datenschutz-Grundverordnung der erhoffte einheitliche und europaweite Rechtsrahmen für den Datenschutz erreicht, der europaweit einen hohen Datenschutzstandard garantiert und kann insbesondere auch das Marktortprinzip Wettbewerbsgleichheit für alle Anbieter, die in Europa ihre Dienste anbieten, sicherstellen?

Mit der Umsetzung der DSGVO ist in jedem Fall das Ziel erreicht, ein im nicht-öffentlichen Bereich weitgehend einheitliches und europaweites Datenschutzrecht zu haben. Die Öffnungsklauseln und Bereichsausnahmen zeigen die mögliche Uneinheitlichkeit auf. Hier können sich die Ausgestaltungen unterschiedlich entwickeln und das Schutzniveau kann auch uneinheitlich werden. Es bleibt die Hoffnung, dass die DSGVO den Rahmen ausreichend datenschutzfreundlich gesteckt hat.

Im öffentlichen Bereich wird es auch weiterhin Unterschiede geben, da die Mitgliedstaaten innerhalb des Rahmens der DSGVO weitgehend frei bleiben, was durchaus zu Unterschieden führen kann. So ist europaweit uneinheitlich, was öffentlich-rechtlich oder privatrechtlich organisiert ist. Deutschland hat beispielsweise öffentlich-rechtlich geregelte soziale Sicherungssysteme, die in anderen Mitgliedstaaten privatrechtlich geregelt sind.

Im Ergebnis wird es daher nur eine weitgehende Vereinheitlichung geben und keine vollständige.

Das Marktortprinzip halte ich grundsätzlich für geeignet, im Bereich des Datenschutzes einen fairen Wettbewerb der Unternehmen in Europa zu erreichen. Die Praxis wird zeigen, ob die Umsetzung der Einforderung der Datenschutzregeln immer so einfach werden wird, denn nicht alle Unternehmen haben einen Standort in Europa oder sind dazu bereit. Dies dürft die Kontrolle sehr erschweren.

Wird die Umsetzung der Datenschutzgrundverordnung gleiche und faire Wettbewerbs-bedingungen für deutsche und europäische Unternehmen sowie US-amerikanischen Unternehmen herstellen?

Auch für die deutschen, europäischen und US-amerikanischen Unternehmen wird der neue Rechtsrahmen mehr Fairness im Wettbewerb im Bereich des Datenschutzes bedeuten. Es wird nicht mehr möglich sein, Geschäftsmodelle außerhalb dieses

neuen Rechtsrahmens in Europa zu etablieren. Hinzu kommen faire Sanktionsmöglichkeiten in Europa, die endlich in ihrer Höhe angemessener sein können und für US-amerikanische Unternehmen nicht ungewohnt sein dürften.

Ein gutes Beispiel für die Akzeptanz des europäischen Datenschutzrechts ist das US-amerikanische Unternehmen Microsoft, das mit dem deutschen Unternehmen T-Systems in Deutschland kooperiert. Der hohe Datenschutzstandard wird von Microsoft durchaus als Wettbewerbsvorteil verstanden.

3) *Welcher Änderungsbedarf ergibt sich aus der Verabschiedung der Datenschutz-Grundverordnung für das deutsche Datenschutzrecht und die zahlreichen bereichsspezifischen Vorgaben?*

Die spezialgesetzlichen Regelungen des öffentlichen Bereichs müssen jetzt vom Bund und von den Ländern auf ihre Kompatibilität mit der DSGVO überprüft werden. Dies ist für die Bundesrepublik Deutschland angesichts der großen Zahl an Normen sicherlich die größte Herausforderung.

Artikel 8 DSGVO regelt die Bedingungen, unter denen die Einwilligung eines Kindes rechtswirksam ist. Die DSGVO lässt den Mitgliedstaaten hinsichtlich des Alters einen eigenen Reglungsspielraum. Sie gibt den Mitgliedstaaten eine Altersspanne von 13 bis 16 Jahren vor. Unterhalb der Altersgrenze ist für die Einwilligung eines Kindes die Zustimmung der Eltern oder aber ersatzweise deren Einwilligung Voraussetzung für die Rechtmäßigkeit der Datenverarbeitung. Die Mitgliedstaaten müssen die Altersgrenze innerhalb des angegebenen Altersbereichs innerstaatlich regeln.

Ein zwingender Anpassungsbedarf besteht für die Mitgliedstaaten im Regelungsbereich der Sanktionen. Zum einen haben Mitgliedstaaten, die bisher für Datenschutzverstöße keine Sanktionsmöglichkeiten vorgesehen haben, nach Art. 79 Ziff. 5 DSGVO ihr Recht im Bereich Sanktionen anzupassen und dies der Kommission entsprechend zu melden. Zum anderen besteht ein zwingender Umsetzungsbedarf auch nach Art. 79 b DSGVO mit der Pflicht zur Regelung der Sanktionen im innerstaatlichen Recht unter der Maßgabe des Art. 79 DSGVO.

Darüber hinaus sind die Datenschutzgesetze im Hinblick auf die Anforderungen an die Einrichtung der Aufsichtsbehörden und in diesem Zusammenhang auch ihre völlige Unabhängigkeit anzupassen. Nicht alle Datenschutzgesetze genügen den Vorgaben der DSGVO.

Wichtig ist die Regelung, wer in Zukunft über die Entsendung der zuständigen Vertretung im Europäischen Datenschutzausschuss entscheiden soll. Hier halte ich die

Konferenz der Datenschutzbehörden selbst für regelungsfähig. Sie hat sich eine Geschäftsordnung gegeben, die auch die Vertretung im Europäischen Datenschutz Ausschuss regeln könnte.

Die Einrichtung einer deutschen Kontaktstelle, die Anlaufstelle im Kohärenzverfahren ist, ist ebenfalls zwingend geboten. Diese Kontaktstelle sollte als Kontaktstelle der Konferenz der Datenschutzbehörden des Bundes und der Länder eingerichtet werden, da dies dem deutschen föderalen System die notwendige Flexibilität geben würde.

Von welchen Öffnungsklauseln sollte der nationale Gesetzgeber zwingend Gebrauch machen, um über die Vorgaben der Datenschutz-Grundverordnung hinausgehende Regelungen zu schaffen?

Der Gesetzgeber sollte von der Öffnungsklausel des Art. 82 DSGVO, der spezifischere Vorschriften für Beschäftigtendaten durch Gesetze oder durch Kollektivvereinbarungen in den Mitgliedstaaten möglich macht, Gebrauch machen. Die Möglichkeit, das Schutzniveaus im Beschäftigtendatenschutz zu verbessern, sollte genutzt werden.

Artikel 80a eröffnet die Freigabe von personenbezogenen Daten in amtlichen Dokumenten, die sich bei öffentlichen Stellen befinden, auf der Grundlage von Unionsrecht oder dem Recht des Mitgliedstaates. Im Kontext mit der DSGVO halte ich entsprechende gesetzliche Regelungen für sinnvoll. Diese könnten in den Informationsfreiheitsgesetzen erfolgen.

In welchen Bereichen besteht zukünftig kein Spielraum mehr für den nationalen Gesetzgeber?

Im Bereich des nicht-öffentlichen Datenschutzes gibt es grundsätzlich nur wenig Regelungsspielraum für die nationalen Gesetzgeber. Genau dies ist das Ziel der DSGVO. Sie will ein weitgehend einheitliches europäisches Recht für den nicht-öffentlichen Bereich schaffen und damit Rechtssicherheit für die Daten verarbeitenden Unternehmen in Europa.

Wo sehen Sie für die nationalen Gesetzgeber nach der Verabschiedung der Datenschutz-Grundverordnung noch Möglichkeiten, Regelungen im nicht-öffentlichen Bereich zu schaffen?

Artikel 6 Abs. 2a i.V.m. Abs. 3 DSGVO ermöglicht den Mitgliedstaaten ausdrücklich die Verabschiedung von spezifischeren Bestimmungen zur Anpassung der Anwendung bzw. Umsetzung von Art. 6 Abs. 1 Ziff. 1c und 1e der DSGVO. Artikel 6 Abs. 1 Ziff. 1c regelt die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung und Ziff. 1e die Verarbeitung personenbezogener Daten für die Wahrnehmung einer im öffentlichen Interesse liegenden

Aufgabe oder in Ausübung öffentlicher Gewalt. Die Mitgliedstaaten können hierfür gesetzliche Regelungen verabschieden, die den Zweck der Datenverarbeitung regeln und die auch Präzisierungen enthalten können. Es besteht aus meiner Sicht sogar die Notwendigkeit, an dieser Stelle auch zukünftig datenschutzrechtliche Regelungen im nicht-öffentlichen Bereich zu verabschieden. Allerdings müssen sich die Regelungen im Rahmen der DSGVO bewegen.

Artikel 20 DSGVO regelt die Zulässigkeit automatisierter Einzelentscheidungen einschließlich Profiling. Nach Abs. 1 hat der Betroffene das Recht, dass ihn betreffende Entscheidungen nicht ausschließlich aufgrund einer automatisierten Einzelentscheidung einschließlich Profiling getroffen werden. Artikel 20 Abs. 2 DSGVO ermöglicht Einschränkungen des Grundsatzes in Abs. 1. Die Mitgliedstaaten können für automatisierte Einzelentscheidungen oder Profiling, die nicht auf eine Einwilligung oder einen Vertragsabschluss, für den sie erforderlich sind, gestützt werden, eigene Rechtsvorschriften erlassen. Diese müssen geeignete Garantien für die Rechte und Freiheiten der betroffenen Person enthalten. Der nationale Gesetzgeber kann also hierzu eigene Regelungen im nicht-öffentlichen Bereich verabschieden. Ein mögliches Beispiel wäre eine Scoring-Regelung.

Ein wichtiger Spielraum ergibt sich in Art. 82 DSGVO für den Bereich der Beschäftigtendaten. Hier können die Mitgliedstaaten durch Gesetz oder durch Kollektivvereinbarungen spezifischere Vorschriften verabschieden.

Artikel 80 Abs. 2 DSGVO ermöglicht Abweichungen oder Ausnahmen von bestimmten Regelungen der DSGVO für die Verarbeitung personenbezogener Daten zu journalistischen Zwecken, zu wissenschaftlichen, künstlerischen oder literarischen Zwecken.

Eine weitere Möglichkeit für die Verabschiedung eigener Regelungen besteht nach Erwägungsgrund Nr. 23a für die Verarbeitung der Daten Verstorbener. Die DSGVO ist auf die Daten Verstorbener selbst nicht anwendbar. Die Regelung von Datenschutzrechten für die Daten Verstorbener kann sowohl im nicht-öffentlichen wie im öffentlichen Bereich sinnvoll sein.

Sehen Sie insbesondere Handlungsbedarf seitens des Gesetzgebers im Bereich der Beschäftigtendaten?

Ja, hier besteht noch immer ein dringender Handlungsbedarf. Der Bereich der Beschäftigtendaten ist in der Bundesrepublik Deutschland in § 32 BDSG geregelt. Er ist im Übrigen ein von der Rechtsprechung geprägter und auch weiter entwickelter Bereich. So wie die DSGVO zu einer Rechtsvereinheitlichung im nicht-öffentlichen Bereich in Europa führt, ist auch im Bereich des Beschäftigtendatenschutzes eine

Rechtsharmonisierung durch den deutschen Gesetzgeber sinnvoll. Eine spezialgesetzliche Regelung kann einen einheitlichen Schutz durch ein hohes Niveau sicherstellen.

Und wenn ja, in welcher Form?

Ich halte die Regelung in einem Beschäftigtendatenschutzgesetz für sinnvoll.

Was kann man außerhalb der Gesetzgebung tun, um den Datenschutz in Umsetzung der DSGVO in Deutschland zu fördern?

Das Thema der „Datensicherheit" spielt heute für einen guten Datenschutz eine herausragende Rolle. Es ist deshalb sinnvoll, die Entwicklung datenschutzfreundlicher Technologien zu unterstützen und Datenschutz als Wettbewerbsfaktor für den Standort Bundesrepublik Deutschland anzuerkennen. Datenschutz wird zunehmend wichtiger werden für Produktentwicklungen.

Ein Bereich, der ebenfalls sehr wichtig ist, ist die Förderung der Entwicklung guter Transparenzmechanismen, nachdem Transparenz von der DSGVO jetzt ausdrücklich geregelt wird. Transparenz ist ein nicht zu unterschätzender Akzeptanzfaktor für die Datenverarbeitung durch die Wirtschaft. Nur wer mit wenigen Worten verständliche Informationen geben kann, wird von den Betroffenen auch verstanden. In diesem Bereich sehe ich noch viel Arbeit, weil die Informationsbedürfnisse unterschiedlich sind und Datenschutz nicht immer leicht verständlich erklärbar sind.

4) *Lässt die Datenschutzgrundverordnung ausreichend Spielraum für Innovation?*

Ganz bestimmt lässt die DSGVO Raum für Innovationen. Gerade im Bereich der datenschutzfreundlichen Technologien sehe ich Spielraum. Wer heute daran arbeitet, Analysemöglichkeiten wie Big Data datenschutzgerecht weiterzuentwickeln, wird die Nase vorn haben. Auch die Arbeit an einer Trusted Cloud ist ein wichtiges Thema.

Leistet sie einen Beitrag dazu, dass Datenschutz sich als Wettbewerbsvorteil für europäische Unternehmen etablieren kann?

Auf jeden Fall leistet die DSGVO einen Beitrag dazu, dass Datenschutz für europäische Unternehmen ein Wettbewerbsvorteil werden kann. Durch die Regelung von „Privacy by Design" beispielsweise werden die Unternehmen angehalten und verpflichtet, Datenschutz in ihren Produkten von vorne herein zu implementieren. Dies ist ein Marktvorteil gegenüber Produkten, die an dieser Stelle erst nachgebessert werden müssen, was häufig mit Kompatibilitätsproblemen verbunden ist,

wenn dritte Firmen dies versuchen. Jede zukünftige Entwicklung sollte deshalb ganz selbstverständlich schon Datenschutzkomponenten enthalten. Auch US-amerikanische Unternehmen arbeiteten im Bereich der datenschutzfreundlichen Technologien. Dies sollte in Deutschland nicht übersehen werden.

Wo und warum sehen Sie in dem neuen Regelungswerk positive und wo negative Effekte für die deutsche und europäische Wirtschaft?

Die Regelung eines „One-Stop-Shop“ sowie einheitliche Datenschutzanforderungen für alle Unternehmen werden mit Sicherheit positive Aspekte für die deutsche und die europäische Wirtschaft haben. Für europäische Unternehmen ist außerdem die Einführung des Marktortprinzips ein großer Vorteil. Hierdurch wird der Wettbewerb mit Unternehmen aus Drittstaaten in Zukunft fairer gestaltet werden. Ein weiter positiver Effekt ist aus meiner Sicht die Regelung von Zertifizierungsverfahren. Zertifizierungen sind geeignet, dem Auftraggeber bei der Vergabe von Unteraufträgen mehr Rechtssicherheit zu geben und gleichzeitig einen hohen Datenschutzstandard zugunsten der Betroffenen umzusetzen. Europäische Datenschutzzertifikate können daher in Zukunft einen Wettbewerbsvorteil darstellen. Die DSGVO kann auch positive Effekte für die Entwicklung von innovativen Produkten haben. Die Anforderungen der DSGVO setzen hier entsprechende Impulse, die genutzt werden müssen.

Negative Effekte sehe ich nicht. Die Annahme, dass die DSGVO im Hinblick auf Big Data Anwendungen und Ubiquitous Computing wirtschaftsfeindlich sei, wird von mir nicht geteilt.

5) *Wie kann man eine flächendeckende Datenschutzaufsicht und -kontrolle im Hinblick auf das in der Verordnung verankerte „One-Stop-Shop“-Verfahren gewährleisten und dabei dem deutschen Föderalismus mit seinen Länderdatenschutzbeauftragten ausreichend Rechnung tragen?*

Die DSGVO ist so gestaltet, dass das „One-Stop-Shop“-Prinzip sowohl in zentralisierten wie auch in föderalen Staaten umgesetzt werden kann. Die Art der Umsetzung in föderal organisierten Mitgliedstaaten obliegt allein den Staaten. Die Bundesrepublik Deutschland ist nicht der einzige föderal organisierte Staat in der Europäischen Union. Auch Spanien ist beispielsweise föderal organisiert. Der „One-Stop-Shop“ ist nach meiner Auffassung in Deutschland unproblematisch umsetzbar. Unternehmen haben für gewöhnlich einen Hauptsitz und deshalb spielt es keine Rolle, ob dieser in einem zentralisierten Mitgliedstaat liegt oder in einem föderalen. Die für den Hauptsitz zuständige Aufsichtsbehörde steht immer fest und

nur diese ist zuständig und trifft Entscheidungen. Damit wird keine Aufsichtsbehörde in ihren räumlichen Kompetenzen negativ berührt.

Tochterunternehmen können bei Konzernen sowohl in anderen Mitgliedstaaten der Europäischen Union als auch im eigenen Land liegen. Auch hier ist die Zusammenarbeit der Aufsichtsbehörden in beiden Fällen unproblematisch möglich.

Welche Möglichkeiten sehen Sie, das innerstaatliche Kooperationsverfahren auszugestalten?

Die Konferenz der Datenschutzbehörden des Bundes und der Länder (DSK) ist ein geeignetes innerstaatliches Gremium für die effektive Umsetzung eines innerstaatlichen Kooperationsverfahrens. Sie kann dafür Sorge zu tragen, dass die deutschen Aufsichtsbehörden einheitlich vorgehen und „mit einer Stimme sprechen". Die Vorgaben der DSGVO sind in dieser Hinsicht klar und werden umgesetzt. Der Konferenz kommt hier eine wichtige koordinierende Aufgabe zu. So wie im Europäischen Datenschutzausschuss, können für die Konferenz im Hinblick auf Mehrheitsentscheidungen keine andern Regelungen gelten. Dies ist sicherlich ein Unterschied zu der derzeitigen Situation, die bisher gar keine gesetzlichen Vorgaben enthält. Allerdings hat sich die Konferenz in einer Geschäftsordnung bereits verbindliche Regelungen gegeben; diese kann die Konferenz entsprechend der Vorgaben der DSGVO zur Umsetzung des Kohärenzmechanismus anpassen.

Um anderen Mitgliedstaaten die Zusammenarbeit mit den vielen Aufsichtsbehörden der Bundesrepublik Deutschland zu erleichtern, ist die Einrichtung einer gemeinsamen Kontaktstelle (die in der DSGVO auch für jeden Mitgliedstaat vorgesehen ist) der DSK besonders wichtig. Diese kann die Weitergabe von Eingaben und Anfragen koordinieren und die Fristenkontrolle übernehmen. Diese kann auch dafür sorgen, Informationen zügig an alle Aufsichtsbehörden in der Bundesrepublik weiterzugeben.

Wie kann die Vertretung der deutschen Datenschutzaufsicht in Brüssel gewährleistet werden, ohne dass eine Doppelvertretung von Bundes- und Landesdatenschutzaufsichtsbehörden erfolgt und wie könnte das Verfahren konkret ausgestaltet werden?

Artikel 46 Abs. 2 DSGVO regelt für den Fall, dass es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde gibt, dass dieser Mitgliedstaat die Aufsichtsbehörde bestimmt, die die Behörden im europäischen Datenschutzausschuss vertritt und dass ein Verfahren eingeführt werden muss, mit dem sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Art. 57 einhalten. Daraus folgt, dass die Bundesrepublik Deutschland von nur einer Aufsichtsbehörde im Europäischen Datenschutzausschuss vertreten wird.

In Erwägungsgrund Nr. 93 der DSGVO wird ausgeführt, dass ein Mitgliedstaat mit mehreren Aufsichtsbehörden sicherstellen soll, dass alle Aufsichtsbehörden am Kohärenzverfahren wirksam beteiligt werden. Daraus folgt keine Vorgabe dafür, welche Aufsichtsbehörde ihren föderalen Mitgliedstaat im Europäischen Datenschutzausschuss vertritt. Dies ist vielmehr innerstaatlich zu regeln.

Die Vertretung der Bundesrepublik Deutschland kann damit grundsätzlich sowohl durch einen Landesbeauftragten als auch durch den Bundesbeauftragten erfolgen. Da im Europäischen Datenschutzausschuss Fälle aus allen Aufsichtsbehörden besprochen und entschieden werden können, kommt es allein darauf an, dass die nötigen Abstimmungen zwischen der in dem Einzelfall zuständigen Aufsichtsbehörde und dem Vertreter im Europäischen Datenschutzausschuss effektiv erfolgen.

Ich halte es für sinnvoll, die detaillierten Regelungen für die deutsche Vertretung im Europäischen Datenschutzausschuss durch eine gesetzliche Regelung der Datenschutzkonferenz in ihrer Geschäftsordnung zu überlassen. Die Bundesrepublik Deutschland ist ein im Föderalismus geübtes Land, so dass diese Aufgabe so wie in den vielen anderen Bereichen auch lösbar ist. Im Vordergrund muss immer stehen, dass die in einem Einzelfall zuständige Aufsicht nach der DSGVO die Verantwortung trägt und sich dies auch im Ausschuss widerspiegeln muss.

Weil die Bundesrepublik Deutschland ein föderales Land ist, sollte trotz nur einer Stimme im Europäischen Datenschutzausschuss immer eine „Doppelvertretung“ durch einen Ländervertreter und den Bund erfolgen. Damit würde sowohl den Bundes- wie auch den Länderinteressen auf faire Weise Rechnung getragen. Auch heute ist ein Ländervertreter neben der Bundesbeauftragten in der Art.29-Gruppe mit anwesend. Trotzdem hat die Bundesrepublik Deutschland nur eine Stimme. Wichtig erscheint mir, dass das Wahlverfahren für das stimmberechtigte deutsche Mitglied im Europäischen Datenschutzausschuss sowie das vertretende Mitglied der Datenschutzkonferenz überlassen wird. Ich kann mir hierfür durchaus eine gesetzliche Vorgabe vorstellen, dass als stimmberechtigtes Mitglied und als Vertretung immer sowohl der Bund als auch ein Land vertreten sein muss.

Der von der in DSGVO vorgesehenen Kontaktstelle kommt für die Bundesrepublik Deutschland auch im Hinblick auf die Vertretung im Europäischen Datenschutzausschuss eine besondere Bedeutung zu. Eine von Bund und Ländern gemeinsam getragene Kontaktstelle, die mit dem nötigen Personal ausgestattet ist, kann gewährleisten, dass jeder von der Datenschutzkonferenz entsandte Vertreter eine solide Arbeitsgrundlage hat und auf erfahrenes und mit der Arbeit vertrautes Personal zurückgreifen kann.

6) *Wie bewerten Sie die DSGVO vor dem Hintergrund des Safe-Harbor-Urteils des EuGH von Oktober 2015 sowie des sogenannten „EU-US Privacy Shield", mit von der Europäischen Kommission ausgehandelten Kontrollbefugnissen und Rechten für europäische Bürger gegenüber amerikanischen Datenverarbeitern, das Anfang des Monats von der KOM vorgestellt wurde?*

Die DSGVO regelt in Kapitel V in den Art. 40 bis 45 die Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen. Die Regelungen der Grundverordnung greifen die bisherigen Regelungen der EU-Datenschutzrichtlinie für Datenübermittlungen in Drittstaaten auf. Eine Änderung der Regelungen aufgrund der Entscheidung des Europäischen Gerichtshofs vom 6. Oktober 2015 zu Safe Harbor ist nicht erfolgt. Demzufolge sind die vom EuGH aufgestellten Voraussetzungen nicht in der DSGVO gesetzlich umgesetzt.

Das von der Kommission in seinen Grundzügen vorgestellte „EU-US Privacy Shield" liegt den Aufsichtsbehörden bzw. der Art.29-Gruppe bisher noch nicht in einer ausformulierten Form zur Prüfung vor. Es ist daher zum jetzigen Zeitpunkt nicht möglich, eine Stellungnahme zu dem „Privacy Shield" als Rechtsgrundlage für Datenübermittlungen an Unternehmen in den USA abzugeben.

7) *Kann Großbritannien tatsächlich eine Ausnahmeregelung in Anspruch nehmen, der zufolge die Sperrklausel des Art. 43a DSGVO bei der Datenübermittlung an Drittstaaten keine Anwendung findet?*

Aus dem Wortlaut der DSGVO in Art. 43a sowie dem Erwägungsgrund Nr. 90 ist nicht unmittelbar ersichtlich, warum diese Sperrklausel zunächst einmal für Großbritannien nicht gelten soll. Allerdings hat Großbritannien offensichtlich in einer Stellungnahme vom 4. Februar 2016 mitgeteilt, dass es von der sogenannten „opt-in" Möglichkeit der Mitgliedstaaten Gebrauch machen werde und seine Einwilligung zur rechtlich bindenden Anerkennung dieser Regelung nicht erteilen werde.

Die Möglichkeit, diese Regelung des Art. 43a nicht anzuwenden, soll für den Bereich Justiz und Inneres, um den es hier geht, in einem sogenannten „opt-in Protokoll" geregelt worden sein, das bedauerlicherweise in den Erwägungsgründen nicht aufgeführt wird. Mir ist diese Möglichkeit bisher nicht bekannt gewesen. Insofern fällt es schwer, sie rechtlich einzuordnen.

Falls ja, wie bewerten Sie diesen Sachverhalt und welche Konsequenzen hätte dies für den Datenaustausch innerhalb von Europa und für britische Unternehmen?

Sollte Art. 43a DSGVO aufgrund eines fehlenden „opt-in“ für Großbritannien nicht anwendbar sein, wären die Folgen gravierend. Zunächst einmal wäre Großbritannien nicht an Art. 43a DSGVO gebunden und könnte in Fallkonstellationen des Art. 43a nach freiem Ermessen oder eigenen Vorschriften Daten in Drittstaaten übermitteln. Dies könnte auch personenbezogene Daten von Europäern oder Dritten betreffen, die in Großbritannien bei dortigen Unternehmen gespeichert werden. Das mit der Aufnahme des Art. 43a bezweckte Ziel, derartige Anfragen noch einmal durch internationale Übereinkünfte rechtsstaatlich abzusichern, würde damit nur noch teilweise erreicht und Großbritannien würde zur Schwachstelle des Systems. Dies würde selbstverständlich auch für andere Mitgliedstaaten gelten, die gegebenenfalls dem Beispiel Großbritanniens folgen.

8) *In Erwägungsgrund 40 wird die Weiterverarbeitung von personenbezogenen Daten für andere Zwecke erlaubt, wenn es sich dabei um eine aufgrund einer Rechtsvorschrift (seitens der Europäischen Kommission oder der Mitgliedsstaaten) „notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses“ handelt. Steht diese Passage vor dem Hintergrund, dass fraglich ist, ob eine einheitliche Rechtsauslegung dieser Begriffe in den Mitgliedsstaaten stattfindet, im Widerspruch zu einem einheitlichen Handeln innerhalb der EU-Mitgliedsstaaten?*

Der Erwägungsgrund 40 stellt klar, dass Mitgliedstaaten die Möglichkeit haben müssen, selbst zu entscheiden, welche Maßnahmen sie zum Schutz der aus ihrer Sicht in ihrem Staat besonders wichtigen Ziele des öffentlichen Interesses für unabdingbar erachten.

Da die Mitgliedstaaten sehr unterschiedlich organisiert sind und die Rechtssysteme nicht einheitlich sind, dürfte diese Befugnis zur Zweckänderung nach den Ratsverhandlungen unausweichlich gewesen sein. Unter dem Gesichtspunkt eines möglichst weitgehenden einheitlichen Datenschutzes ist dies bedauerlich; doch ich befürchte, die dahinterstehende Unterschiedlichkeit der Rechtssysteme der einzelnen Mitgliedstaaten hat hier tatsächlich keine andere Lösung zugelassen. Aus Sicht des Datenschutzes wäre selbstverständlich eine einheitliche Reglung besser gewesen.

9) *Wie bewerten Sie die Ausnahmen der DSGVO zur Rechtmäßigkeit von Datenverarbeitung ohne Einwilligung zu Zwecken von berechtigtem Interesse?*

Artikel 6 Abs. 1 Ziff. f DSGVO erlaubt die Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten unter der Voraussetzung, dass die Interessen, Grundrechte oder

Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Dies gilt insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Diese Regelung entspricht in ihren wesentlichen Elementen dem heutigen § 28 Abs. 1 Ziff. 2 des Bundesdatenschutzgesetzes. Hinzugekommen ist die ausdrückliche Nennung von Kindern in der Interessenabwägung.

Aus Art. 6 Abs. 1 Ziff. f DSGVO letzter Satz ergibt sich, dass die Regelung nicht für von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitungen gilt.

Auslegungsbedürftig ist der Begriff der berechtigten Interessen, der grundsätzlich eine Privilegierung der Daten verarbeitenden Stelle mit sich bringt. Die Notwendigkeit unbestimmter und damit auslegungsbedürftiger Rechtsbegriffe ist zunächst einmal nicht von der Hand zu weisen.

Nach Erwägungsgrund 38 kann die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden. Allerdings sehe ich diese einseitige Privilegierung der Direktwerbung, wie sie dem Erwägungsgrund beispielhaft zu entnehmen ist, kritisch. Auch hier ist immer eine Abwägung im Einzelfall erforderlich, um zu klären, ob die berechtigten Interessen des Betroffenen nicht zurückzustehen haben. Die Interessenabwägung kann daher als Korrektiv gesehen werden. Nach Erwägungsgrund 57 sollen Betroffene in Fällen, in denen ihre Daten verarbeitet werden, um Direktwerbung oder eine mögliche spätere Verarbeitung einschließlich Profiling zu betreiben, hiergegen zumindest jederzeit unentgeltlich Widerspruch einlegen können.

Der Erwägungsgrund 38a DSGVO benennt als weiteres mögliches berechtigtes Interesse die Verarbeitung von personenbezogenen Daten innerhalb einer Unternehmensgruppe für interne Verwaltungszwecke, einschließlich Kunden- und Beschäftigtendaten. Damit privilegiert der Erwägungsgrund Unternehmensgruppen und auch Konzerne. Unberührt bleiben die Regelungen für Datenübermittlungen in Drittstaaten.

Die pauschale Privilegierung von Kunden- und Beschäftigtendaten sehe ich durchaus kritisch. Auch hier kommt es in der Praxis darauf an sicherzustellen, dass weiterhin eine Abwägung im Einzelfall mit den Interessen, Grundrechten oder Grundfreiheiten der betroffenen Person erfolgt. An dieser Stelle sollte es Aufgabe des Europäischen Datenschutzausschusses sein, für eine grundrechtskonforme Anwendung zu sorgen.

In Erwägungsgrund 39 wird die Verarbeitung zu Zwecken der Gewährleistung der Netz- und Informationssicherheit als ein berechtigtes Interesse ausgeführt. Auch

hier - und gerade hier - muss in jedem Einzelfall eine Interessenabwägung vorgenommen werden. Hier stehen sich wichtige unterschiedliche Rechtsgüter gegenüber und eine einfache pauschale Antwort wird es nicht geben. Ich gehe davon aus, dass der Europäische Datenschutzausschuss hier ebenfalls ein Working-Paper erarbeiten wird, um die Fallkonstellationen zu systematisieren und Anwendungshilfen für die Abwägungen im Einzelfall zu geben.

Kleinmachnow, den 19. Februar 2016

Dagmar Hartge

Die Landesbeauftragte für den Datenschutz und
für das Recht auf Akteneinsicht Brandenburg